					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P18S					Tytuł dokumentu: **Polityka zabezpieczeń kryptograficznych**							
Wersja: 1.0		Data wejścia w życie: 01.01.2025			Właściciel dokumentu:							
X	Polityka		Standard		Procedura		Formularz		Rejestr		Inne	

Historia zmian				
Numer zmiany	**Data zmiany**	**Zmiany**	**Przegląd wykonał**	**Właściciel procesu**

Zatwierdzenia			
Imię i nazwisko	**Stanowisko**	**Data**	**Podpis**

Dostosowanie do norm i regulacji

Norma/regulacja	Klauzula/artykuł	Komentarz
ISO/IEC 27001:2022	Klauzula 8	
ISO/IEC 27002:2022	Środki kontrolne 8.24, 8.25	
NIST SP 800-53 Rev. 5	SC-12 do SC-17	
Dyrektywa NIS2	Artykuły 21(2)(d), 21(2)(e)	
Rozporządzenie DORA	Artykuły 6(2)(d), 9(2)(f)	
COBIT 2019	DSS05.01, APO13	
RODO	Artykuły 32(1)(a), 34	

1. Cel

1.1 Niniejsza polityka określa obowiązkowe wymagania dotyczące stosowania szyfrowania i zabezpieczeń kryptograficznych w celu zapewnienia poufności, integralności i autentyczności danych biznesowych oraz danych osobowych.

1.2 Zapewnia właściwe stosowanie mechanizmów kryptograficznych w systemach, na urządzeniach oraz w usługach chmury obliczeniowej w środowisku małej organizacji.

1.3 Niniejsza polityka bezpośrednio wspiera certyfikację ISO/IEC 27001:2022 oraz pomaga organizacji spełniać obowiązki prawne wynikające z RODO, dyrektywy NIS2 oraz rozporządzenia DORA.

1.4 Zakres niniejszej polityki obejmuje w szczególności szyfrowanie danych, zarządzanie certyfikatami, bezpieczne postępowanie z kluczami oraz szyfrowanie kopii zapasowych.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do:

2.1.1 wszystkich pracowników, kontrahentów i stron trzecich przetwarzających dane organizacji,

2.1.2 wszystkich systemów biznesowych, punktów końcowych i platform chmurowych wykorzystywanych do przechowywania, przesyłania lub uzyskiwania dostępu do informacji poufnych,

2.1.3 wszelkich danych osobowych, finansowych, prawnych lub innych informacji wrażliwych sklasyfikowanych zgodnie z Polityką klasyfikacji danych i etykietowania,

2.1.4 wszelkich zabezpieczeń kryptograficznych, w tym metod szyfrowania, kluczy, haseł, certyfikatów i modułów bezpieczeństwa.

2.2 Polityka obejmuje dane w spoczynku, dane w tranzycie oraz dane przetwarzane. Reguluje również szyfrowanie stosowane w odniesieniu do kopii zapasowych, poczty elektronicznej, zewnętrznych transferów danych oraz publicznie dostępnych witryn internetowych.

3. Cele

3.1 Zapewnienie, aby informacje wrażliwe i podlegające regulacjom były przez cały czas chronione z zastosowaniem odpowiednich środków kryptograficznych.

3.2 Określenie odpowiedzialności za dobór narzędzi szyfrujących, ich konfigurację oraz zarządzanie kluczami.

3.3 Zapobieganie nieuprawnionemu dostępowi, manipulacji oraz wyciekom danych przez stosowanie bezpiecznych mechanizmów transmisji i przechowywania.

3.4 Spełnienie wymagań prawnych i regulacyjnych nakazujących szyfrowanie danych osobowych i danych biznesowych.

3.5 Utrzymanie bezpieczeństwa operacyjnego i dostępności przez skuteczne zarządzanie certyfikatami i kluczami kryptograficznymi.

4. Role i odpowiedzialności

4.1 GM

4.1.1 Zatwierdza niniejszą politykę i zapewnia stosowanie wymagań dotyczących zabezpieczeń kryptograficznych.

4.1.2 Dokonuje przeglądu odstępstw, zgłoszeń naruszeń oraz zgodności dostawców z wymaganiami dotyczącymi szyfrowania.

4.1.3 Weryfikuje, czy usługi outsourcingowe lub usługi chmurowe spełniają wymagane standardy szyfrowania.

4.2 Dostawca usług wsparcia IT / wewnętrzny administrator IT

4.2.1 Wdraża i utrzymuje rozwiązania szyfrujące (np. szyfrowanie pełnodyskowe, certyfikaty SSL/TLS, VPN).

4.2.2 Zarządza cyklem życia kluczy kryptograficznych oraz mechanizmami ich bezpiecznego przechowywania.

4.2.3 Konfiguruje i monitoruje szyfrowanie w celu ochrony kopii zapasowych, witryn internetowych i urządzeń.

[... Sekcje 4.3–8 nie są uwzględnione w tej wersji zapoznawczej. Zakup pełny dokument, aby uzyskać dostęp do pełnej treści. ...]

9. Wymagania dotyczące przeglądu i aktualizacji

9.1 Coroczny przegląd

9.1.1 Niniejsza polityka musi być poddawana przeglądowi co najmniej raz w roku przez GM we współpracy z Dostawcą usług wsparcia IT oraz Koordynatorem ds. prywatności.

9.2 Przesłanki przeglądu doraźnego

9.2.1 Przeglądy muszą być również przeprowadzane, jeżeli:

9.2.1.1 zmienią się standardy lub protokoły kryptograficzne (np. wycofanie algorytmu),

9.2.1.2 zostaną wdrożone nowe systemy lub usługi chmurowe,

9.2.1.3 naruszenie lub incydent dotyczy naruszonego klucza lub certyfikatu,

9.2.1.4 zmiany prawne lub regulacyjne wpływają na wymagania dotyczące szyfrowania.

9.3 Kontrola wersji i komunikacja

9.3.1 Wszystkie zmiany polityki muszą być dokumentowane w rejestrze historii wersji.

9.3.2 Personel musi zostać poinformowany o aktualizacjach, a poprzednie wersje muszą być archiwizowane.

9.3.3 Najnowsza zatwierdzona wersja musi być przechowywana w centralnym repozytorium polityk.

10. Powiązane polityki i zależności

10.1 Niniejszą politykę należy stosować łącznie z następującymi politykami SME:

10.1.1 P12S – Polityka zarządzania aktywami: zapewnia stosowanie szyfrowania do sklasyfikowanych aktywów podczas przechowywania, transferu i utylizacji.

10.1.2 P14S – Polityka retencji danych i utylizacji: określa okresy przechowywania i wymaga szyfrowanego przechowywania danych do czasu ich bezpiecznego usunięcia.

10.1.3 P17S – Polityka ochrony danych i prywatności: zapewnia zgodność szyfrowania z zasadami ochrony danych oraz wymaganiami regulacyjnymi wynikającymi z art. 32 RODO.

10.1.4 P22S – Polityka rejestrowania i monitorowania: wymaga rejestrowania użycia kluczy, awarii szyfrowania oraz wygaśnięcia certyfikatów na potrzeby audytu.

10.1.5 P30S – Polityka reagowania na incydenty: określa procedury eskalacji, powstrzymania i powiadamiania w przypadku nieskuteczności szyfrowania lub naruszenia kluczy.

11. Normy referencyjne i ramy odniesienia

11.1 ISO/IEC 27001

11.1.1 Klauzula 8.1 – wymaga wdrożenia zabezpieczeń operacyjnych, w tym szyfrowania, w celu zarządzania ryzykiem bezpieczeństwa.

11.2 ISO/IEC 27002

11.2.1 Środek kontrolny 8.24 – określa wymagania dotyczące stosowania szyfrowania w celu zapewnienia poufności i integralności.

11.2.2 Środek kontrolny 8.25 – określa zasady bezpiecznego zarządzania kluczami kryptograficznymi i certyfikatami.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SC-12 – określa wymagania dotyczące ustanawiania kluczy kryptograficznych i ich walidacji.

11.3.2 SC-13 – definiuje standardy generowania kluczy kryptograficznych.

11.3.3 SC-17 – obejmuje infrastrukturę klucza publicznego (PKI) oraz zarządzanie cyklem życia certyfikatów.

11.3.4 SC-28 – wymaga szyfrowania danych w spoczynku.

11.3.5 SC-12 do SC-17 (rodzina) – zapewnia prawidłowe wdrożenie ochrony kryptograficznej w systemach.

11.4 RODO

11.4.1 Artykuł 32(1)(a) – wymaga wdrożenia środków technicznych, takich jak szyfrowanie, w celu zapewnienia poufności danych.

11.4.2 Artykuł 34 – wskazuje, że szyfrowanie może zwolnić organizację z obowiązku powiadamiania o naruszeniu, jeżeli dane były niezrozumiałe dla osób nieuprawnionych.

11.5 Dyrektywa NIS2

11.5.1 Artykuł 21(2)(d) – wymaga skutecznego szyfrowania w celu zabezpieczenia systemów i komunikacji.

11.5.2 Artykuł 21(2)(e) – podkreśla ochronę danych i ograniczanie cyberzagrożeń przez stosowanie szyfrowania.

11.6 Rozporządzenie DORA

11.6.1 Artykuł 6(2)(d) – wymaga, aby systemy ICT utrzymywały bezpieczne kanały komunikacji oraz szyfrowanie.

11.6.2 Artykuł 9(2)(f) – zobowiązuje podmioty finansowe do stosowania silnego szyfrowania w celu ochrony komunikacji cyfrowej i wymiany danych.

11.7 COBIT 2019

11.7.1 DSS05.01 – wymaga ochrony informacji wrażliwych przez szyfrowanie i protokoły kryptograficzne.

11.7.2 APO13.02 – wymaga skutecznego wdrożenia środków bezpieczeństwa, w tym zabezpieczeń kryptograficznych, jako elementu planowania bezpieczeństwa informacji.